EXHIBIT 12

Original

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All Content and Other Information Associated with the Email Account

[redacted]

Maintained at Premises Controlled by Microsoft Corporation, and the Email Accounts

[redacted]

Maintained at Premises Controlled by Google LLC, USAO Reference No. 2019R00949

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

20 MAG 4007

Agent Affidavit in Support of Application for Search Warrants for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

ELIZABETH A. KUDIRKA, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am a sworn officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated by 18 U.S.C.

BitMEX has U.S. Customers

12. From my review of a spreadsheet obtained from BitMEX pursuant to a grand jury subpoena, and a production letter from BitMEX counsel accompanying that document, I know that, despite prior public claims to the contrary, and despite IP address controls and other checks that BitMEX has put in place over time purportedly to identify U.S. customers and prevent them from trading on BitMEX, BitMEX in fact serviced many U.S.-based customers during the time that it lacked any registration status with the CFTC. For example, as of March 7, 2019, BitMEX had identified approximately 434 customers who had traded on the BitMEX platform and who either self-disclosed as U.S. persons or who BitMEX identified as U.S. persons through internet protocol ("IP") address and manual checks. The spreadsheet includes the email address of each identified U.S. user, and includes email addresses with ".edu" extensions associated with United States colleges and universities. The spreadsheet reflects a total of 347.98 Bitcoin in net revenue earned by BitMEX from the 434 identified U.S. traders. From my review of Bitcoin-USD exchange rates available at https://www.xe.com/currencycharts/?from=XBT&to=USD&view=1Y, I know that on March 7, 2019, 1 Bitcoin closed with a value of $3,851.62 USD. Accordingly, as of March 7, 2019, the Bitcoin earned by BitMEX from the 434 identified U.S. users was worth approximately $1,340,289.71 USD.

BitMEX is Not CFTC Registered and Lacks Adequate Controls

13. From my review of the transcript of a deposition that the CFTC took of Arthur Hayes in or about July 2019 (the "Hayes Deposition"), I know that neither BitMEX nor any of its affiliated entities have ever applied to become registered in any capacity with the CFTC.

has had asterisks next to the fields for entering a user's email address, password, and country (or region) of residence, but no asterisks appear next to the fields for first and last name. From my prior experience with websites and electronic forms, I understand that asterisks are typically used to denote mandatory fields, such that the lack of an asterisk next to the first and last name fields on the BitMEX registration page indicates that those fields were not and are not mandatory.

16. From my review of the transcript of a deposition that the CFTC took of Greg Dwyer in or about April 2019 (the "Dwyer Deposition"), I know the following facts, among others:

a. Dwyer began working at BitMEX in late 2015. He was the first employee of BitMEX aside from its three co-founders: Arthur Hayes, Sam Reed, and Ben Delo. Dwyer started with BitMEX as the head of business development has during his tenure also supervised customer support. Until the beginning of 2019, Dwyer worked for BitMEX from New York. Before joining BitMEX, Dwyer worked and shared an apartment with Hayes.

b. From the time that Dwyer joined BitMEX in or about 2015 through the date of his CFTC deposition in or about April 2019, BitMEX did not collect know-your-customer documents when individuals registered for BitMEX accounts and only took steps to verify customer identification if an account was compromised or lost access.[1] As Dwyer described, a customer only needs a first name and last name, an email address, and a password to register for

[1] When asked about know your customer policies during the Hayes Deposition, Hayes claimed that BitMEX has "risk-based" know-your-customer policies and procedures in which "certain actions by users or customers will trigger [BitMEX] to ask for additional information before they are allowed to continue[] operating on the platform." Hayes claimed that these risk-based policies are triggered in three specific circumstances: (1) if a customer is flagged as coming from a restricted jurisdiction and challenges that designation; (2) if a customer loses their two-factor authentication code; and (3) if one of the BitMEX founders in reviewing customer withdrawal activity notices "something out of place." Hayes acknowledged that this process did not apply to all customer accounts and nowhere claimed that BitMEX collected or verified accountholder identification across its customer base – data integral to the assessment of risk associated with a particular customer in a "risk-based" KYC program.

BitMEX, but BitMEX does not take steps upon signup to check the first and last name provided against any form of identification. From the information described above, Dwyer appears to be mistaken about the fact that BitMEX users needed a first and last name to register with the platform.

17. In or about November 2019, I interviewed a former BitMEX employee ("Witness- 1")[2]. During those interviews, Witness-1 stated the following, in substance and in part:

a. Witness-1 is a former employee of BitMEX. In Witness-1's role at BitMEX, Witness-1 was familiar [redacted] Witness-1 was first in communication with employees of BitMEX beginning in or about [redacted] and has been in contact with BitMEX employees and/or customers throughout [redacted]

b. During Witness-1's tenure at BitMEX, BitMEX did not have formal know your customer verification upon customer registration and only attempted to verify accountholder identification in limited situations such as when a customer lost their two-factor authentication or for email changes; BitMEX did not have anti-money laundering policies or controls; BitMEX did not file suspicious activity reports (or "SARS") with the U.S. government; and BitMEX did not have policies or procedures for identifying transactions subject to U.S. sanctions.

B. Probable Cause Regarding the Subject Accounts

18. As detailed below, there is probable cause to believe that each of the Subject Accounts is used by a U.S.-based user of a BitMEX trading account and will contain evidence of BitMEX's violation of the BSA through the offer or sale of its futures products to U.S. customers.

[2] Witness-1 is cooperating with the Government's investigation [redacted]. Further, Witness-1 may face criminal exposure for obstruction; no promises regarding leniency as to any potential charges have been extended to Witness-1.

BitMEX Account Email Addresses

19. From my review of the BitMEX website and a user data spreadsheet produced by BitMEX, which according to BitMEX counsel reflects BitMEX user data available as of January 15, 2020, I know that in order to register for an account on BitMEX, a customer must provide a verified email address. Accordingly, each BitMEX customer account has an email address associated with it.

20. From my review of email communications obtained from customers of BitMEX, I have learned that BitMEX uses a customer's registered email address to communicate with the customer, including by sending automated messages about activity on the customer's account to that address. For example, BitMEX sends emails to its customers notifying of account logins and withdrawal activity that reflect the IP addresses that the customer uses to conduct that activity. These emails have included messages sent to BitMEX customers listing IP addresses that are geographically located in the United States. From my training and experience in investigations involving electronic evidence, I know that IP addresses can be run against public databases to identify the geographic location associated with a particular IP address. This geographic location information cannot be relied upon entirely to determine where a person—such as a BitMEX customer—is located. For example, Virtual Private Network or "VPN" services allow a user to mask their true IP address and to instead access the internet from a different IP address associated with a different geographic location. Nevertheless, emails from BitMEX to its customers notifying them that they are accessing BitMEX from an IP address that is geographically located in the United States indicates either that a BitMEX customer is in fact located in the United States (in violation of BitMEX's purported U.S. user ban) or that the customer is using a VPN to pretend to